REMARKS

Applicants respectfully request reconsideration as follows:

The rejection of claims 14, 16, 21 and 23-25 as being anticipated by Kitamura (USP 6,816,948).

Consider the embodiments disclosed by the Applicants. For example, in one embodiment, the Applicants have provided a block-level storage device that responds to secure write commands as discussed with regard to Figure 3: the host encrypts data 300 according to a content key 305. The storage device stores the resulting encrypted content 310 onto the storage medium 25. However, the content key 305 is encrypted according to a session key by the host and transmitted to the storage device. The storage device decrypts the content key 210 and re-encrypts the content key using a hard disk drive (HDD) key 230 that is never revealed to the host. The storage device then writes the encrypted content key 307 to the storage medium.

In this embodiment, the linkage between the metadata (the content key) and the data is maintained by the host. However, the Applicants disclosed a more sophisticated storage device that, although it responds to block level requests for content, has knowledge of the file system used by the host such that the storage device can identify the necessary metadata corresponding to stored content. (see, e.g., page 20, line 13 – page 22, line 17).

Claim 14 is directed to a system that includes such a "smart" block-level storage device . For example, claim 14 requires the host to "identify the file system object to the storage device if the requested file system object comprise secure content." The corresponding storage engine within the storage device is configured "to respond to block-level requests from the host system by retrieving the content at the requested block addresses from the storage medium, the storage engine being further configured to access the security metadata if the block-level requests correspond to content comprising a secure file system object."

Kitamura stands in sharp contrast to such a system. In particular, there is no security metadata associated with file system objects whatsoever in Kitamura. Instead, as discussed with regard to Figures 1 and 3, Kitamura's storage device has an access list

(element 500 of Figure 3). Each host is assigned a port ID. Depending upon a host's port ID, that particular host has access to certain portions of the storage medium. For example, the host at port ID 00 has access to blocks 0 through 100. The host at port ID 01 has access to blocks 1000 through 5000. But note that the Kitamura storage device has no knowledge whatsoever of file system object security metadata. Instead, all the Kitamura storage device knows is that a certain host can access a certain portion of its storage medium.

In sharp contrast, claim 14 requires that the storage engine "to access the security metadata if the block-level requests correspond to content comprising a secure file system object." The Kitamura device doesn't know the difference between secure and non-secure content. Morover, the Kitamura makes no suggestion for a storage engine that will recognize secure file system object requests (even though the content is requested on a block level) and access the corresponding security metadata. As discussed by the Applicants on pages 22 and 23, the resulting "smart" storage engine can then manage metadata such as copy flags, play counters, locked/unlocked flags, and other features. Such advantages are in no way suggested or taught by Kitamura.

Accordingly, claim 14 and its dependent claims 15-22 are abundantly patentable over Kitamura.

Applicants disclosed further refinements. For example, as discussed on page 28 of the specification, a "hybrid" storage device is disclosed that implements a file system for encrypted file system objects. In this fashion, the storage engine will store secure file system objects and the associated security metadata in a manner of its own choosing. For non-secure file system objects, the storage device responds in a conventional block-level fashion. This is advantageous because of the large bandwidth of block-level drivers in host devices. Claim 23 is directed to such an advantageous system in that the host is configured "to request for non-secure file system objects by identifying the block addresses corresponding to the non-secure file system object and to request for secure file system objects by identifying the file system object." The corresponding storage engine is configured to "respond to block to respond to block-level requests for non-secure file system objects by translating the block-level requests from the host system to byte-level

offsets within a file system object on the storage medium, the storage engine being further configured to control the file system associated with secure file system objects by determining where secure file system objects will be stored on the storage medium and where the corresponding security metadata will be stored on the storage medium."

Kitamura doesn't even disclose or suggest the less sophisticated system of claim 14, let alone the hybrid system of claim 23 (in which the host accesses non-secure file system objects through block level requests and accesses secure file system objects by identifying the file system object and in which the storage engine performs the translation for the block level requests and then controls the manner in which secure file system objects and their security meta-data will be stored). Accordingly, claim 23 and its dependent claims 24 – 28 are patentable over Kitamura.

The rejection of claims 15, 17-21, 27 and 28 as being unpatentable over Kitamura in view of Ta (USP 7,168,787) and the rejection of claim 22 as being unpatentable over Kitamura in view of Okaue (USP 7,124,436)

Neither Ta nor Okaue does anything to cure the infirmities of the primary Kitamura reference. Accordingly, the pending claims are allowable over the art of record.

If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

Certificate of Facsimile Transmission

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date shown below.

_____
Jonathan Hallman
Date of Signature: April 30, 2008

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicant(s)
Reg. No. 42,622
Customer No. 32,605